

# EXHIBIT B

# US 8,099,368 B2 Claim chart VS FiServ

The following claim chart **does not** include, rely or refer to Google Pay, Samsung Pay or Apple Pay, for infringement.

# U.S. Patent No. US 8,099,368

**US8099368B2**  
United States

[Download PDF](#)
[Find Prior Art](#)
[Similar](#)

**Inventor:** Todd R. Coulter, Mordechai E. Kaplinsky, Christopher E. Lewis

**Current Assignee :** Authwallet LLC

---

**Worldwide applications**

2009 • [US](#) [US](#)

---

**Application US12/557,457 events** ⓘ

- US case filed in California Northern District Court ⓘ
- US case filed in Texas Southern District Court ⓘ
- US case filed in Texas Northern District Court ⓘ
- US case filed in Texas Northern District Court ⓘ

**2008-11-08** • Priority to US11274908P

**2009-09-10** • Application filed by FonWallet Transaction Solutions Inc

2009-09-10 • Priority to US12/557,457

2009-11-06 • Priority claimed from PCT/US2009/063641

2010-03-24 • Assigned to FONWALLET TRANSACTION SOLUTIONS, INC. ⓘ

**2010-05-13** • Publication of US20100121767A1

2010-08-18 • Priority claimed from US12/859,203

2010-08-18 • Priority claimed from US12/859,205

2010-08-18 • Priority claimed from US12/859,213

**2012-01-17** • Publication of US8099368B2

**2012-01-17** • Application granted

2020-03-06 • Assigned to AUTHWALLET LLC ⓘ

2022-02-08 • Assigned to AUTHWALLET LLC ⓘ

2022-08-12 • US case filed in Texas Northern District Court ⓘ

**Status** • Active

**2029-09-10** • Anticipated expiration

Claims priority from a provisional application: 11/08/2008

Total patent Term Adjustments 0

# US 8,099,368 : Claim 1

A method for processing financial transaction data in a server including a processor and an associated storage area, the method comprising:

receiving from a requester an authorization request generated as a result of a transaction at a point of purchase, wherein the authorization request includes a purchaser identifier, a transaction amount, and information identifying the point of purchase;

authenticating the authorization request;

retrieving customer information associated with the purchaser identifier from the storage area, the customer information including data defining multiple payment instruments and an address associated with a mobile device of the customer;

generating a transaction indication message for transmittal to the mobile device of the customer, the transaction indication message including information about the transaction and specifying a response that allows a selection of a payment instrument from at least two of the multiple payment instruments associated with the customer;

transmitting the transaction indication message to the mobile device using the mobile device address;

receiving a customer confirmation message from the mobile device in response to the transaction indication message, wherein the customer confirmation message includes a selected payment instrument;

obtaining customer account information from an issuing institution, wherein the customer account information includes information associated with the selected payment instrument from the multiple payment instruments associated with the customer, the customer account information including a first part encrypted according to a first encryption method and a second part encrypted according to a second encryption method, the first encryption method and the second encryption method selected such that the server is capable of decrypting the first part and is not capable of decrypting the second part; and

providing the customer account information to the requester in response to determining that the customer confirmation message indicates that the transaction is authorized by the customer.

# US 8,099,368 : Claim 21

A method for processing financial transaction data in a server including a processor and a memory, the method comprising:

by the processor, receiving an initial authorization request to receive credit for purposes of a transaction, wherein the initial authorization request includes transaction information and a customer identifier,

retrieving customer information from the memory based on the customer identifier, wherein the customer information includes payment instrument information defining multiple payment instruments and customer device information specifying a contact address associated with a customer device;

sending a transaction notification to the contact address associated with the customer device, wherein the transaction notification includes data from the transaction information and information that allows a consumer to select a payment instrument from at least two of the multiple payment instruments associated with the customer,

receiving a confirmation message from the customer device, wherein the confirmation message includes a selection of an individual payment instrument from the multiple payment instruments, and

generating an information request to receive account information for a payment instrument based on the initial authorization request, the customer information, and the selected individual payment instrument;

sending the information request to an issuer,

receiving account information from the issuer, the account information including a first part encrypted according to a first encryption method and a second part encrypted according to a second encryption method, the first encryption method and the second encryption method selected such that the server is capable of decrypting the first part and is not capable of decrypting the second part;

and

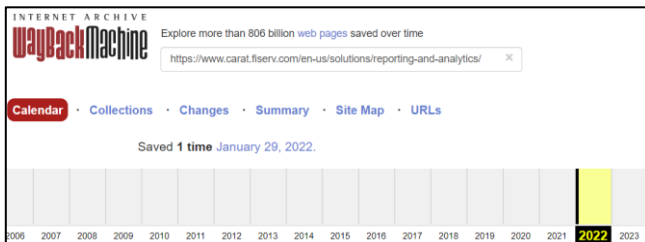
providing the account information to a requester.

# US 8,099,368 : Claim 1

1. A method for processing financial transaction data in a server including a processor and an associated storage area, the method comprising:

Fiserv processes financial transaction data to administer the authorization request processing stream in programmatic payments and many other services. A processor and a storage area are required to perform these methods.

<https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/>

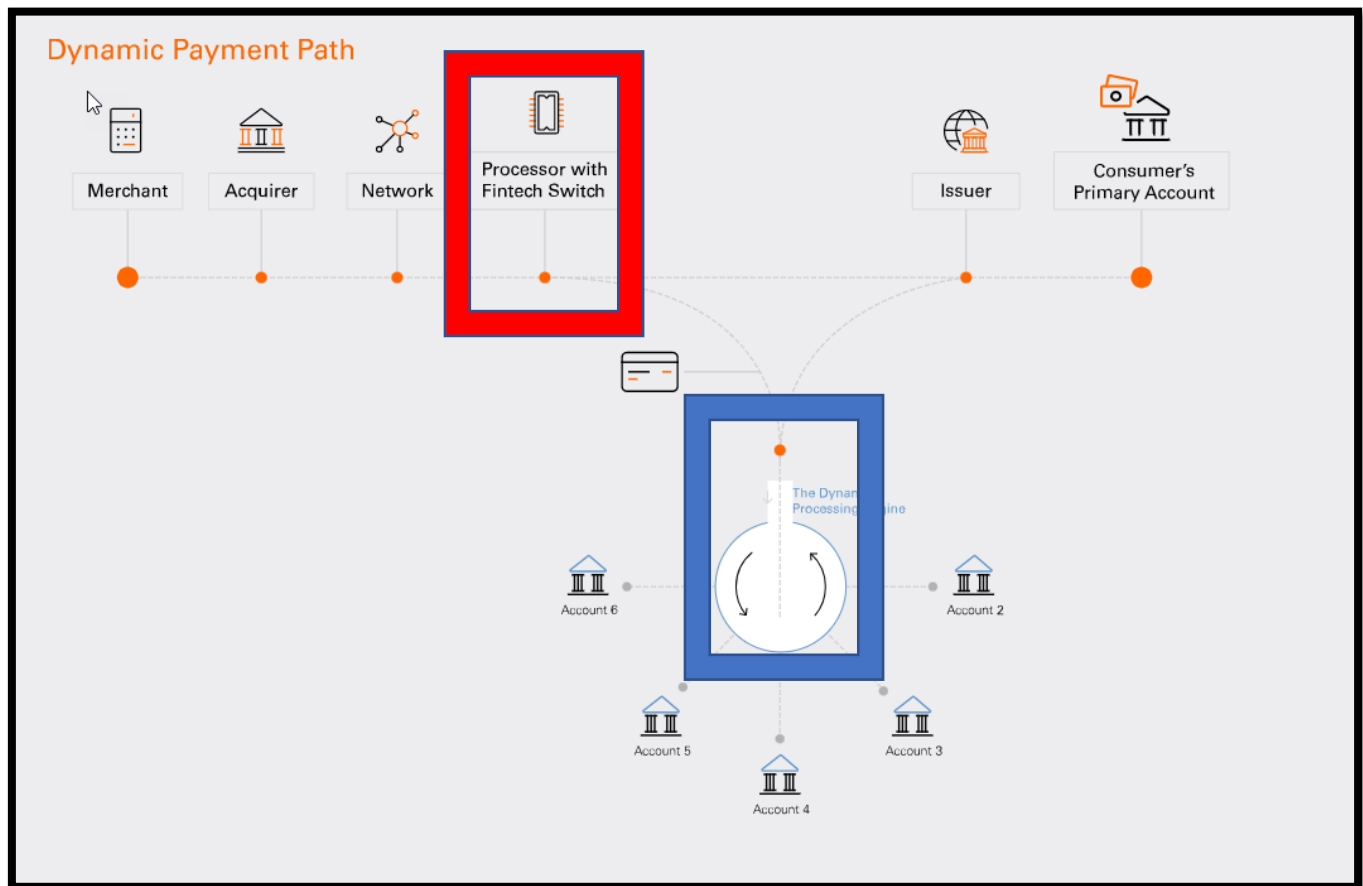


[http://web.archive.org/web/2022000000000\\*/https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/](http://web.archive.org/web/2022000000000*/https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/)

# US 8,099,368 : Claim 1

receiving from a requester an authorization request generated as a result of a transaction at a point of purchase, wherein the authorization request includes a purchaser identifier, a transaction amount, and information identifying the point of purchase;

Fiserv receives the authorization request message (ISO-8583) at its intermediary, which Fiserv calls the Fintech switch. The AUTH request includes track 1 & 2 data which defines both the transaction and customer information.

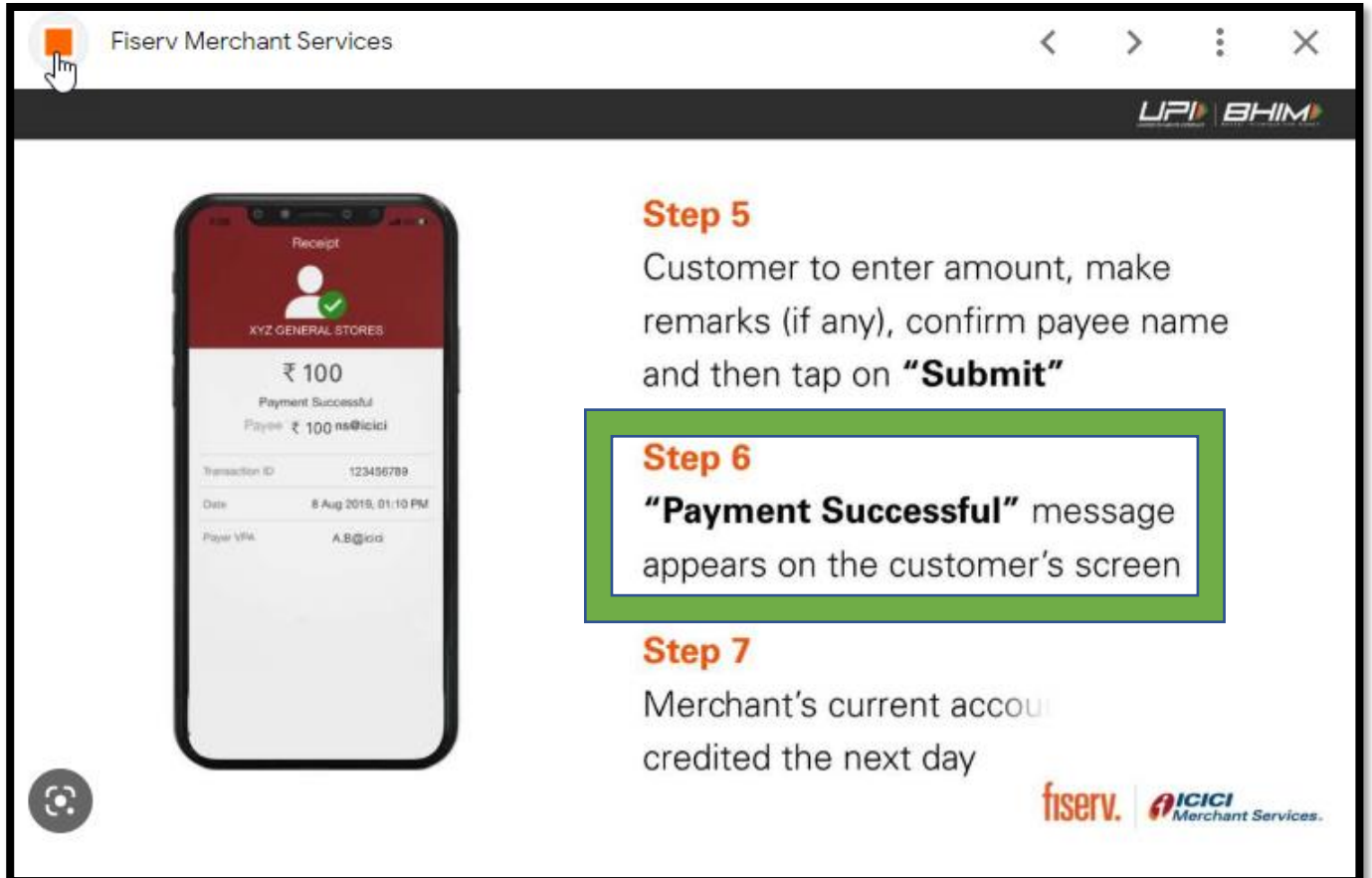


<https://www.fiserv.com/en/about-fiserv/the-point/understanding-programmable-payments.html>

# US 8,099,368 : Claim 1

authenticating the authorization request;

The **customer confirms a selected payment method via a received confirmation message from the customer.**



<https://merchants.fiserv.com/india/resources-support/>



[https://web.archive.org/web/20230000000000\\*/https://merchants.fiserv.com/india/resources-support/](https://web.archive.org/web/20230000000000*/https://merchants.fiserv.com/india/resources-support/)



# US 8,099,368 : Claim 1

retrieving customer information associated with the purchaser identifier from the storage area, the customer information including data defining multiple payment instruments and an address associated with a mobile device of the customer;

FiServ fintech switch receives an authorization request, which identifies the customer / purchaser identifier. Fiserv then finds account including each payment method and contact information to reach the accounts assigned mobile device

## Unlock revenue through innovation

Collaborate with our global and local experts to imagine and realize new customer experiences. Explore recent innovations in OSR, Grocery, Insurance, and Petro.

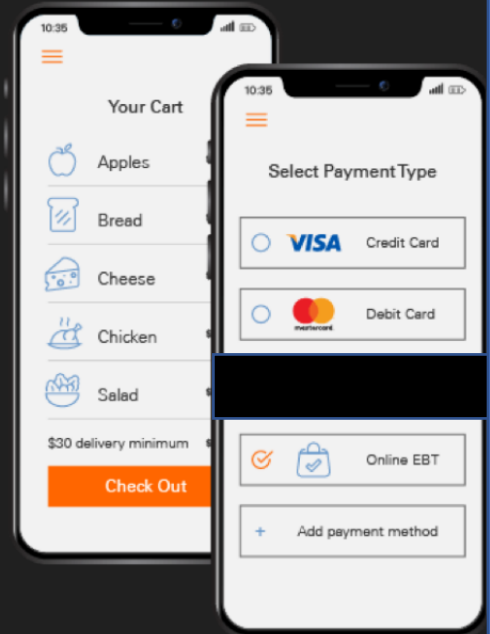
Contact Us

### Localized Promotions

#### Safer Orders

Grocers are accepting Online EBT across 45 states<sup>1</sup>

#### Voice Commerce



<https://cld-stage-carat.fiserv.com/en-us/>

# US 8,099,368 : Claim 1

generating a transaction indication message for transmittal to the mobile device of the customer, the transaction indication message including information about the transaction and specifying a response that allows a selection of a payment instrument from at least two of the multiple payment instruments associated with the customer;

Fiserv developer studio gives the ability to look up account information and access customer information – including customer payment method details.

The screenshot displays the Fiserv Developer Studio interface. On the left, a sidebar menu lists various API categories, with 'Information Lookup' and its sub-item 'Card Info Lookup' highlighted by a red rectangle. The main content area shows the 'Internet Payment Gateway (IPG) NA' section, specifically the 'Card Info Lookup' endpoint. The endpoint is marked as 'ACTIVE' and version '1.0.0 (latest)'. The method is 'POST' and the path is '/card-information'. A description states: 'Use this to look up card related information such as issuer country, card function and card brand.' Below this, 'Additional resources' include links to 'Download API specifications' and 'Download Postman collection'. At the bottom, there are tabs for 'Parameters', 'Request Schema', 'Response Schema', and 'Response Codes'. On the right, a 'Code Snippet' panel shows a JSON response for a successful request, including fields like 'storeId', 'paymentCard', 'expiryDate', 'securityCode', 'bic', 'bankCode', 'cardFunction', 'cardholderName', 'bin', 'last4', and 'brand'.

<https://developer.fiserv.com/product/IPGNA/api/?type=post&path=/card-information&branch=main&version=1.0.0>

# US 8,099,368 : Claim 1

transmitting the transaction indication message to the mobile device using the mobile device address;

A transaction request is sent to the customer notifying customer of transaction. Also, enabling payment method selection



<https://www.carat.fiserv.com/en-us/solutions/encryption-and-tokenization/>

# US 8,099,368 : Claim 1

receiving a customer confirmation message from the mobile device in response to the transaction indication message, wherein the customer confirmation message includes a selected payment instrument;

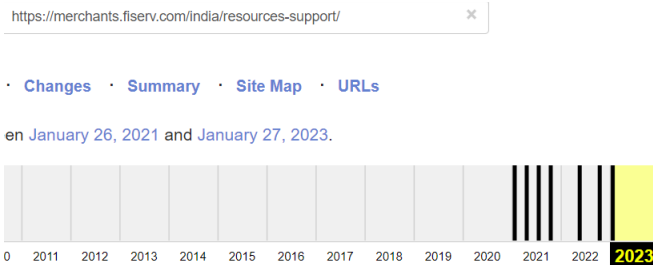
The **customer confirms a selected payment method via a received confirmation message from the customer.**

The screenshot displays the Fiserv Merchant Services interface. On the left, a mobile device screen shows a 'Receipt' from 'XYZ GENERAL STORES' for a payment of ₹ 100. The receipt includes details: Transaction ID 123456789, Date 8 Aug 2019, 01:10 PM, and Payer VPA A.B@icici. On the right, the interface provides instructions for the merchant:

- Step 5**: Customer to enter amount, make remarks (if any), confirm payee name and then tap on **"Submit"**
- Step 6**: **"Payment Successful"** message appears on the customer's screen
- Step 7**: Merchant's current account credited the next day

The interface also features logos for UPI, BHIM, fiserv, and ICICI Merchant Services.

<https://merchants.fiserv.com/india/resources-support/>




[https://web.archive.org/web/20230000000000\\*/https://merchants.fiserv.com/india/resources-support/](https://web.archive.org/web/20230000000000*/https://merchants.fiserv.com/india/resources-support/)

# US 8,099,368 : Claim 1

obtaining customer account information from an issuing institution, wherein the customer account information includes information associated with the selected payment instrument from the multiple payment instruments associated with the customer, the customer account information including a first part encrypted according to a first encryption method and a second part encrypted according to a second encryption method, the first encryption method and the second encryption method selected such that the server is capable of decrypting the first part and is not capable of decrypting the second part; and


Fiserv encrypts data and enables cardholder data to be decrypted depending who is authorized and owns the keys.

Carat offers multiple layers of security to help safeguard cardholder data at every stage of the payment process. Together with EMV®, part of your payment acceptance solution, it provides a multilayered, end-to-end approach:




### Encryption

Protecting cardholder data in transit from the swipe of the card until it reaches Fiserv secure data center.



### Tokenization

Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent – referred to as a token – that has no external meaning or value.



### EMV

Chip-based technology reduces the risk of accepting counterfeit cards in face-to-face transactions. PIN-enabled cards reduce the risk of counterfeiting, and misuse of lost or stolen cards.

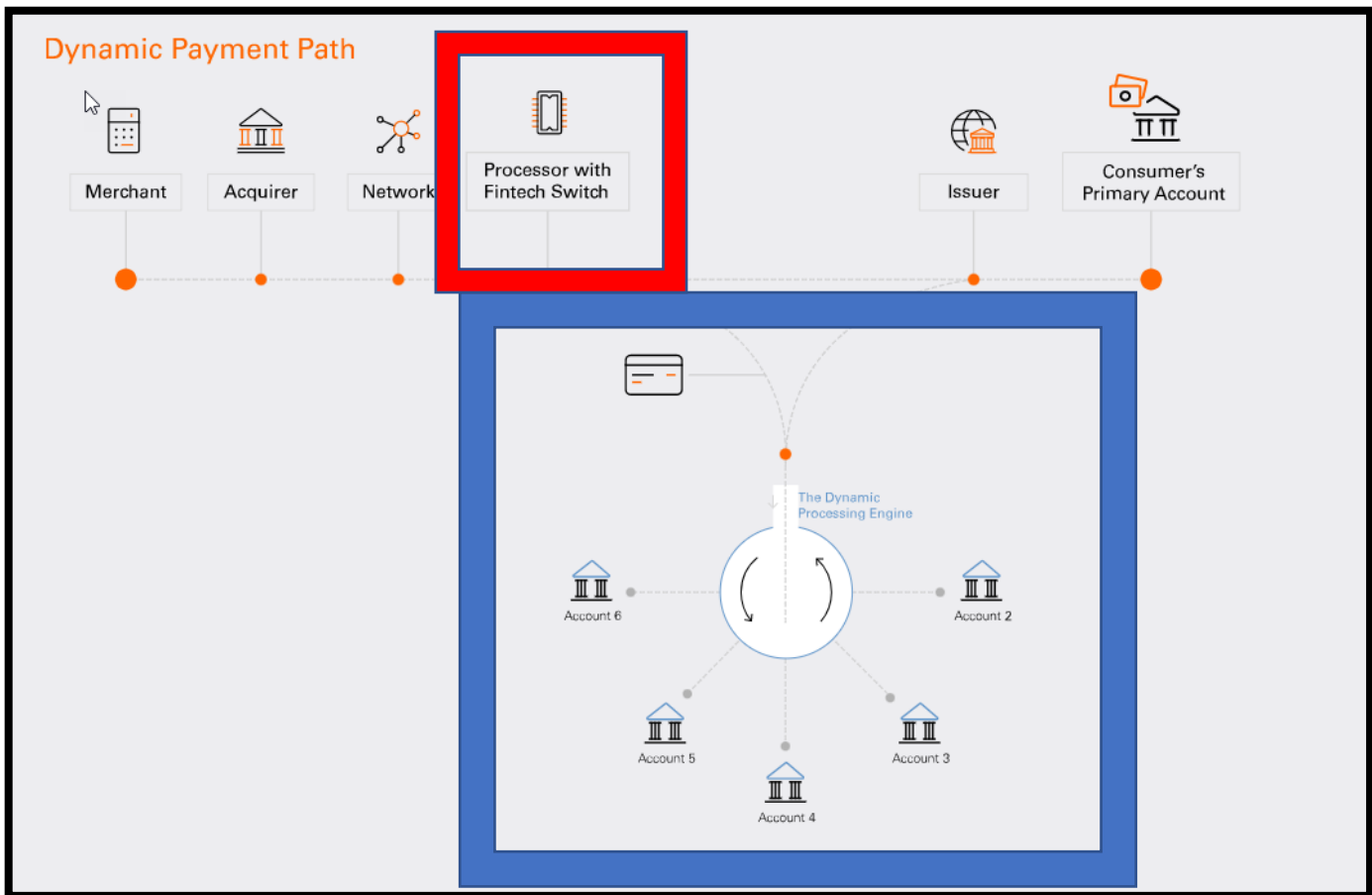
Contact your **Carat Relationship Manager** today for more information.

**Carat**

# US 8,099,368 : Claim 1

providing the customer account information to the requester in response to determining that the customer confirmation message indicates that the transaction is authorized by the customer.

The Fiserv fintech switch (intermediary) sends the data to and from the various accounts that request payments.



<https://www.fiserv.com/en/about-fiserv/the-point/understanding-programmable-payments.html>

# US 8,099,368 : Claim 21

A method for processing financial transaction data in a server including a processor and a memory, the method comprising:

Fiserv processes financial transaction data to administer the authorization request processing stream in programmatic payments and many other services. A processor and a storage area are required to perform these methods.

Save Time and Effort

Reduce Fraud Risk and Expense

Understand Global Omnichannel Activity

Lower Development Costs

Better Interchange and Fee Visibility

## Streamline Transaction Management

Access and manage business-critical data through a one-stop, omnichannel platform. Better understand every stage of

Transaction Activity  
Review critical processing metrics.

Authorization Summary

ClientLine

Home

MONITORING

Authorizations

Sites

uCom

Lobby

REPORTS

Authorizations

uCom

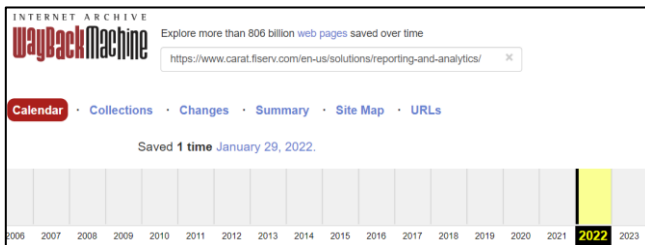
Authorized Sales #  
1,906,639  
(1,906,639) (+14.87%)

Show Details

As Compared To Previous 7 days

Sales (USD)

<https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/>

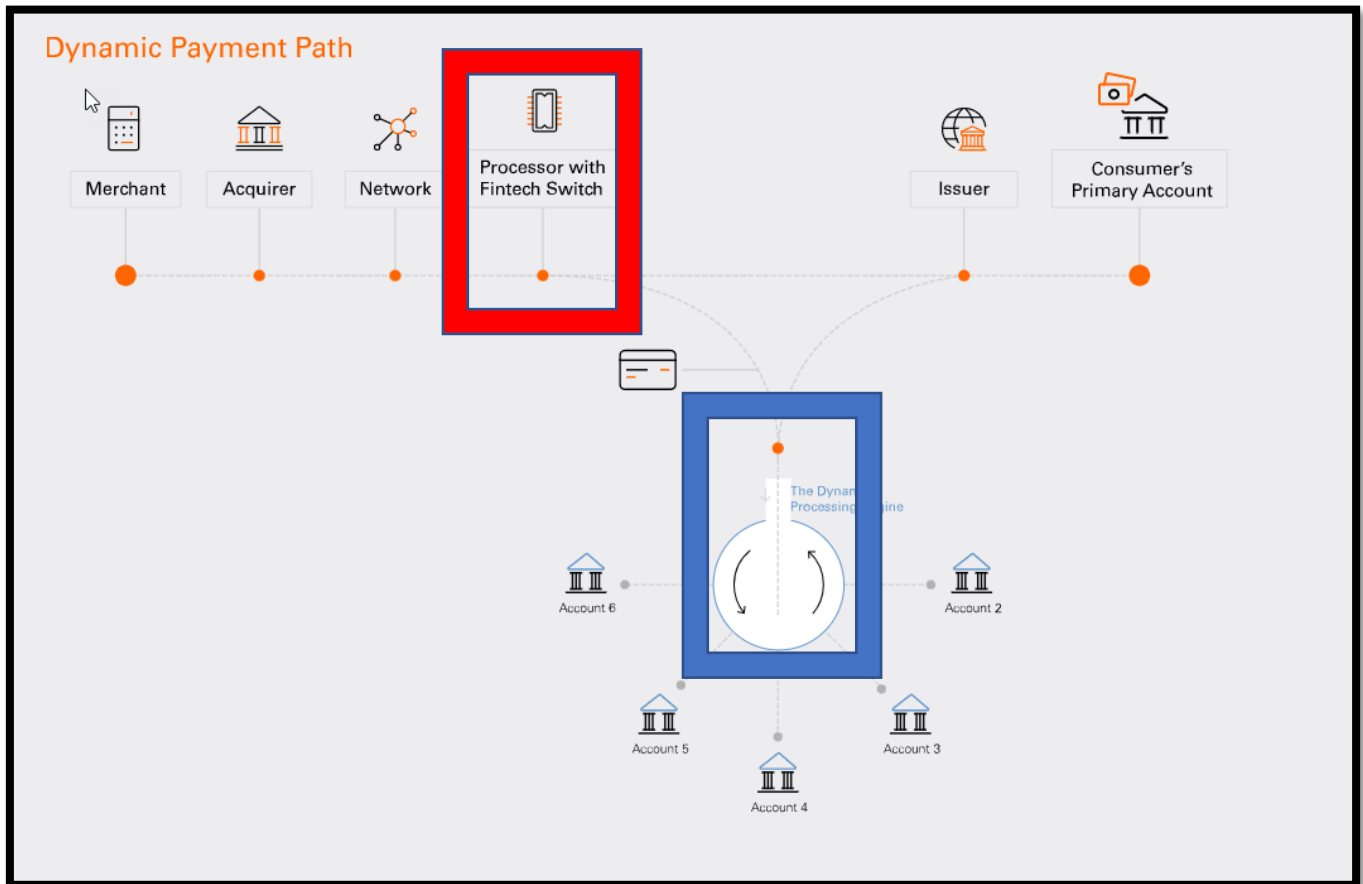


[http://web.archive.org/web/2022000000000\\*/https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/](http://web.archive.org/web/2022000000000*/https://www.carat.fiserv.com/en-us/solutions/reporting-and-analytics/)

# US 8,099,368 : Claim 21

by the processor, receiving an initial authorization request to receive credit for purposes of a transaction, wherein the initial authorization request includes transaction information and a customer identifier,

Fiserv receives the authorization request message (ISO-8583) at its intermediary, which Fiserv calls the Fintech switch. The AUTH request includes track 1 & 2 data which defines both the transaction and customer information.



<https://www.fiserv.com/en/about-fiserv/the-point/understanding-programmable-payments.html>



# US 8,099,368 : Claim 21

retrieving customer information from the memory based on the customer identifier, wherein the customer information includes payment instrument information defining multiple payment instruments and customer device information specifying a contact address associated with a customer device;

**FiServ fintech switch receives an authorization request, which identifies the customer / purchaser identifier. Fiserv then finds account including each payment method and contact information to reach the accounts assigned mobile device**

## Unlock revenue through innovation

Collaborate with our global and local experts to imagine and realize new customer experiences. Explore recent innovations in OSR, Grocery, Insurance, and Petro.

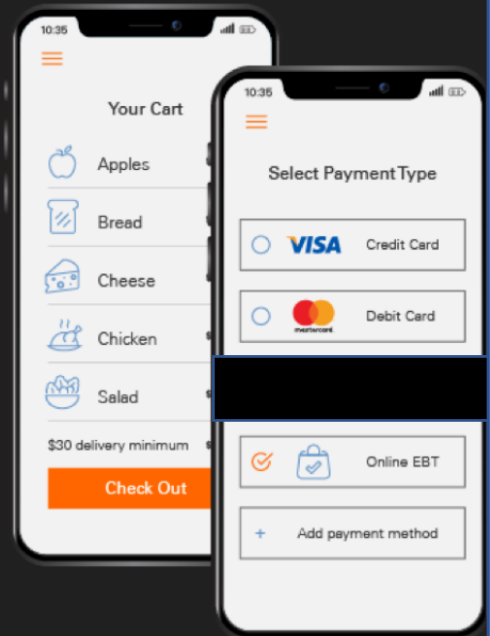
Contact Us

### Localized Promotions

#### Safer Orders

Grocers are accepting Online EBT across 45 states<sup>1</sup>

#### Voice Commerce



<https://cld-stage-carat.fiserv.com/en-us/>

# US 8,099,368 : Claim 21

sending a transaction notification to the contact address associated with the customer device, wherein the transaction notification includes data from the transaction information and information that allows a consumer to select a payment instrument from at least two of the multiple payment instruments associated with the customer,

A transaction request is sent to the customer notifying customer of transaction. Also, enabling payment method selection



<https://www.carat.fiserv.com/en-us/solutions/encryption-and-tokenization/>

# US 8,099,368 : Claim 21

receiving a confirmation message from the customer device, wherein the confirmation message includes a selection of an individual payment instrument from the multiple payment instruments, and

The **customer confirms a selected payment method via a received confirmation message from the customer.**

The screenshot displays the Fiserv Merchant Services interface. On the left, a smartphone screen shows a payment receipt for XYZ GENERAL STORES, indicating a successful payment of ₹ 100 via ICICI. The receipt includes transaction details such as Transaction ID, Date, and Payer VPA. On the right, three steps are outlined:

- Step 5:** Customer to enter amount, make remarks (if any), confirm payee name and then tap on **"Submit"**
- Step 6:** **"Payment Successful"** message appears on the customer's screen
- Step 7:** Merchant's current account credited the next day

The interface also features logos for UPI, BHIM, fiserv, and ICICI Merchant Services.

<https://merchants.fiserv.com/india/resources-support/>

<https://merchants.fiserv.com/india/resources-support/>

· [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

en January 26, 2021 and January 27, 2023.



[https://web.archive.org/web/20230000000000\\*/https://merchants.fiserv.com/india/resources-support/](https://web.archive.org/web/20230000000000*/https://merchants.fiserv.com/india/resources-support/)

# US 8,099,368 : Claim 21

generating an information request to receive account information for a payment instrument based on the initial authorization request, the customer information, and the selected individual payment instrument;

Fiserv developer studio gives the ability to look up account information and access customer information – including customer payment method details.

The screenshot displays the Fiserv Developer Studio interface. The top navigation bar includes the Fiserv logo, 'Developer Studio', and links for 'Sign in' and 'Create account'. A sidebar on the left lists various API categories, with 'Information Lookup' highlighted. The main content area shows the 'Internet Payment Gateway (IPG) NA' product page, specifically the 'Card Info Lookup' endpoint. The endpoint is marked as 'ACTIVE' and version '1.0.0 (latest)'. The method is 'POST' and the path is '/card-information'. A description states: 'Use this to look up card related information such as issuer country, card function and card brand.' Below this, there are links for 'Download API specifications' and 'Download Postman collection'. On the right, a 'Code Snippet' section shows a JSON request body for a card lookup, with a 'Run Request' button. The JSON body includes fields like 'storeId', 'paymentCard' (with 'number', 'expiryDate', 'month', 'year'), 'securityCode', 'bic', 'bankCode', 'cardFunction', 'cardHolderName', 'bin', 'last4', and 'brand'.

<https://developer.fiserv.com/product/IPGNA/api/?type=post&path=/card-information&branch=main&version=1.0.0>

# US 8,099,368 : Claim 21

sending the information request to an issuer,

the information request is sent to the card issuer / bank to receive specific requested information,

The screenshot shows the Fiserv Developer Studio interface. The top navigation bar includes the Fiserv logo, 'Developer Studio', and links for 'Sign in' and 'Create account'. Below this is a secondary navigation bar with 'Who we serve', 'Search', 'Catalog', and 'Support'. The main content area is titled 'Exchange' and 'Information Retrieval'. A left sidebar lists various API categories, with 'Information retrieval' highlighted. The main content area contains a section for 'Bank Retrieval' with a detailed description of the API request and response.

**Exchange** **ACTIVE**

**Information Retrieval**

**Bank Retrieval**

The Bank Details for a Merchant that is boarded on the system under the PayFac can be retrieved using the `/account/bank-details` request. The `merchant_id` used must be a billing or funding level node for the merchant (that holds a bank), otherwise an error with explanation: "Invalid Merchant ID provided, node is not billing or funding" will be returned. For billing and funding levels on the subgroup and merchant level, the `internal_mid` for the node may be used.

<https://developer.fiserv.com/product/Exchange/docs/?path=docs/getting-started/information-retrieval.md>

# US 8,099,368 : Claim 21

receiving account information from the issuer, the account information including a first part encrypted according to a first encryption method and a second part encrypted according to a second encryption method, the first encryption method and the second encryption method selected such that the server is capable of decrypting the first part and is not capable of decrypting the second part; and

Fiserv encrypts data and enables cardholder data to be decrypted depending who is authorized and owns the keys.

Carat offers multiple layers of security to help safeguard cardholder data at every stage of the payment process. Together with EMV®, part of your payment acceptance solution, it provides a multilayered, end-to-end approach:



## Encryption

Protecting cardholder data in transit from the swipe of the card until it reaches Fiserv secure data center.



## Tokenization

Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent – referred to as a token – that has no external meaning or value.



## EMV

Chip-based technology reduces the risk of accepting counterfeit cards in face-to-face transactions. PIN-enabled cards reduce the risk of counterfeiting, and misuse of lost or stolen cards.

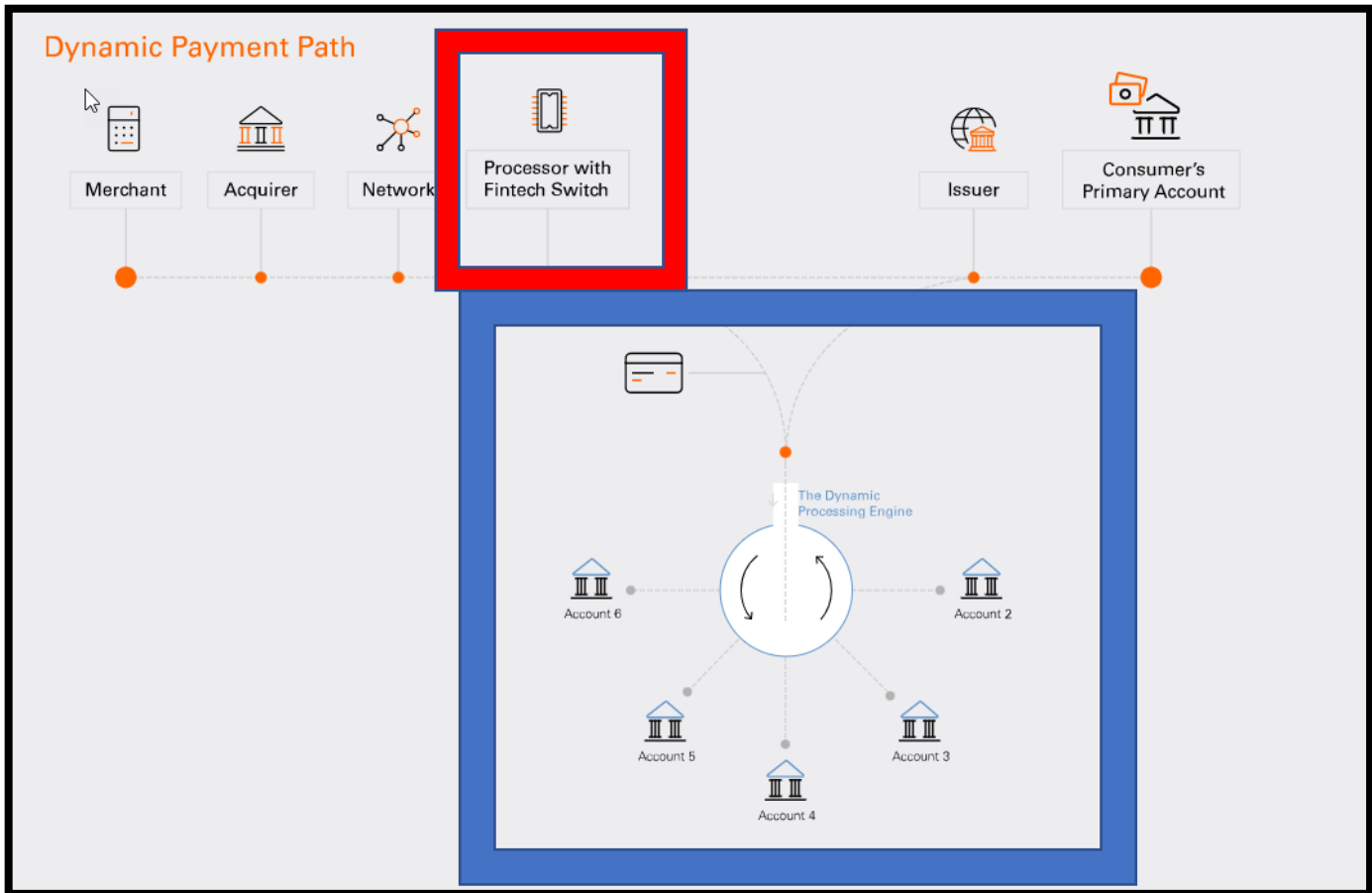
Contact your [Carat Relationship Manager](#) today for more information.

**Carat**

# US 8,099,368 : Claim 21

providing the account information to a requester.

The Fiserv fintech switch (intermediary) sends the data to and from the various accounts that request payments.



<https://www.fiserv.com/en/about-fiserv/the-point/understanding-programmable-payments.html>